Implementing Number Matching in MFA Applications

October 2022

OVERVIEW

CISA is releasing this fact sheet to highlight threats against accounts and systems using mobile push-notification-based multifactor authentication (MFA). Mobile push-notification-based MFA is a form of application-based MFA that authenticates via a mobile application notifying a user's smart phone. After receiving the prompt (aka "push" notification), the user presses "approve" on the notification to grant themselves access to their account. Cyber threat actors can gain access to systems with mobile push-notification-based MFA through using the "MFA fatigue" technique. MFA fatigue, also known as "push bombing," occurs when a cyber threat actor bombards a user with mobile application push notifications until the user either approves the request by accident or out of annoyance with the nonstop notifications.

To protect against MFA fatigue as well as other attack vectors such as phishing, CISA strongly encourages all organizations to implement phishing-resistant MFA, as detailed in CISA fact sheet Implement Phishing-Resistant MFA to Protect Against Cyber Threats. (**Note:** The Office of Management and Budget requires agencies to adopt phishing-resistant MFA methods.) If an organization that uses mobile push-notification-based MFA is unable to implement phishing-resistant MFA, CISA recommends using number matching to mitigate MFA fatigue. Although number matching is not as strong as phishing-resistant MFA, it is the best interim mitigation for organizations who may not immediately be able to implement phishing-resistant MFA.

MULTIFACTOR AUTHENTICATION PROMPTS

Mobile-push-notification-based MFA uses "push" notifications to alert a user to review a new MFA authentication request. The login flow is:

1. The user enters their username and password to authenticate.
2. The identity platform sends a signal to the app on the user's phone, which generates a notification.
3. The user opens and accepts the prompt to approve the request.

Figures 1 and 2 show how these prompts appear in Microsoft Authenticator.

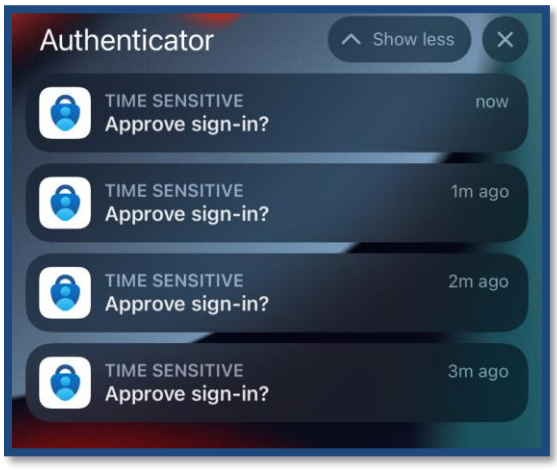

Figure 1: Microsoft Authenticator "Push" Notifications

Figure 2: Microsoft Authenticator Prompt Approval

THE PROBLEM

Cyber threat actors who have obtained a user's password know they can enter it into an identity platform that uses mobile-push-notification-based MFA to generate hundreds of prompts on the user's device over a short period of time.[1] This activity understandably annoys the user, who may—accidentally or from MFA fatigue—press accept to stop the prompts. Alternatively, the prompts may confuse the user, who may assume one of the requests is legitimate and approve. As a result of any of these possible scenarios, the user unknowingly grants the cyber threat actor access to their account:

MITIGATION

As stated above, if an organization that uses mobile push-notification-based MFA is unable to implement phishing-resistant MFA, CISA recommends enabling "number matching" on MFA configurations to prevent MFA fatigue. Number matching is a setting that forces the user to enter numbers from the identity platform into their app to approve the authentication request. Figures 3 and 4 provide the user's view of an identity platform login screen that uses number matching.

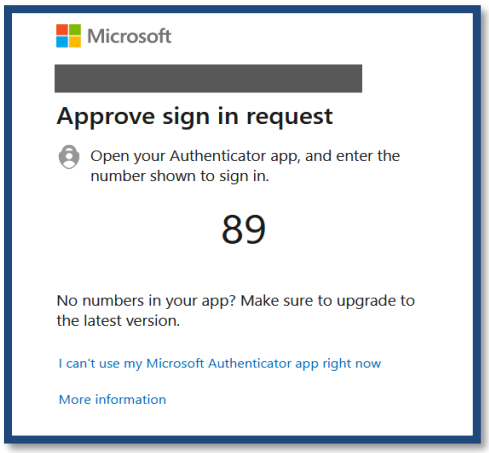

Figure 3: Azure AD Number Matching Prompt

Figure 4: Microsoft Authenticator Number Matching Prompt

The number matching requirement mitigates MFA fatigue by:

- **Requiring access to the login screen to approve requests**. Users cannot approve requests without entering the numbers on the login screen.
- **Discouraging prompt spam**. A threat actor does not benefit from generating many authentication prompts as each prompt requires the user to enter a unique set of numbers that only the threat actor would have.

MFA vendors support number matching features under a variety of brand names. A few common examples:

- **Microsoft Number Matching** – Use number matching in multifactor authentication (MFA) notifications (Preview) - Azure Active Directory - Microsoft Entra | Microsoft Docs
- **Duo Verified Push** – Duo Administration - Policy & Control | Duo Security
- **Okta TOTP** – https://help.okta.com/oie/en-us/Content/Topics/identity-engine/authenticators/configure-okta-verify-options.htm

[1] Threat actors could acquire a user's password via password spraying, a password dump from a compromised site, or other methods.

Disclaimer: The United States Government through the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security (DHS) does not endorse any commercial product or service. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise is provided for informational purposes and does not constitute or imply their endorsement, recommendation, or favoring by CISA or DHS.

BEST PRACTICES FOR USING MFA WITH NUMBER MATCHING

Train users to report. In addition to implementing the mitigations noted above, CISA recommends training users to report unknown or bulk confirmation requests. Organizations should provide periodic cybersecurity training that includes:

- MFA fatigue,
- How to recognize MFA spam
- How to report unknown confirmation request

Investigate denied push notifications. CISA recommends that organizations investigate denied push notification request occurrences. When a user denies an MFA requests, they should alert their IT security team, who should investigate the root cause. MFA checks are done after the first factor (e.g., the user's password) is satisfied, so denied MFA requests could mean the user's password is compromised.